# ACCÈS SSH

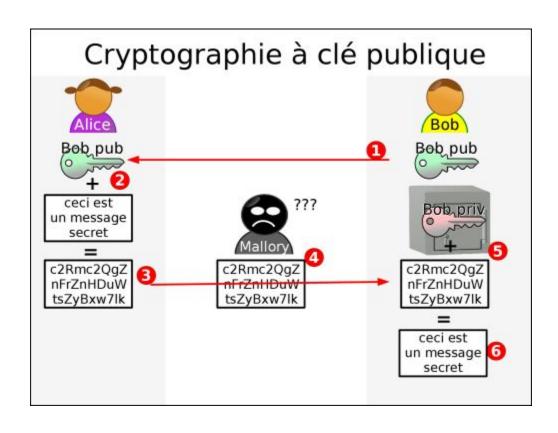
Où l'on accèdera à son système à distance

# QU'EST CE QUE SSH?

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

## COMMENT MARCHE LA CRYPTOGRAPHIE À CLEF PUBLIQUE?



### POURQUOI ÇA MARCHE DANS UN SENS ET PAS DANS L'AUTRE?



#### privkey.asc

-----BEGIN PGP PRIVATE KEY BLOCK-----

TO REST TOTAL OF A CHARGE VALUE OF THE STATE mc@sBroUR#ESeANmCoLdilgoOju4mdJWcC/cGRhF/HsFoof2X9vLWveqHLOlciY BEhyloTUlKeBY79EM84IS7w81JS3ro7GPi/rB05EEusNBOoMaDKe4W8Ey514u145 CLIBDIAVBIAWBIA VAMANA O BOLLONDO ANTHOGETUBI (QAENCCOGTI TAVAMO I LORVONETU ALTYNDOJOBSYMIGETPOPATUBIANI/VEYTRANIARTYKI PI JA /WENOTELIJINODI TOUDO WYTCOBYNDOSTA/EDLANIADOKSEDYK/TRANIARTYKI PI JA /WENOTELIJINODI COMDE Mg-db6PwinLuUkAY-GT6STOUSDON/TIVKLblCvh8KZaccOBKI pilcvi7QARAQAD aSC4ioTuRAPlyMat9fe+8XhRifd2k3E78cHFCay94019uUHBTCHDFHCyBCywiM mhCv4ZJUzHBrOFufsoeYn/JITwzEkbObPdsFDzXRZ+UzSFwuCWrelCPTt4aJCi0 nev zemzveni i sastavitetuni volustekolov kriti i ar odi viteva-o i i popula kasekseko Oppeziotte o ozofi kohndul annohi (Wakitzari projekta) and Podrypanuli kati UVI fretuoriki Projektikori kritikori volustikori (Aliani, Indonesia) voluska (a Pinola iliutaki visikki yenki jari olustikori oloshitati (ryti Tityappeti suvikifi di pili kati yukit isti Sityaki voluski kritikori oloshitati (ryti Tityappeti XIII oloshitati UE2EARAAvUDSlaung-1LumEJcOx2+nCv-(VOAGex70muvoFJX1HbLoGPEohtEIOR) oGA#zOci2DeLOc4inrS2X50XS5cETOFr3uFDBOO+USFcXXE1vaRiVxv3B3FLo4F yJatAGF5yydHkD6h0Qq2bPdT11kKttHBk2iLWnniyoReSuUyArfAev/y9e1BG7F hEV:00MSe0CuXL/SGcongsDdAmsZ/pClS4CtSwkSe4esne07eYWs5n1snJsOv904 z8kbhGtmNvLHZJO9EJ86bWN4gf8pni54Bb30d1WI3iL38hbKzvStLRUviVp7KeSi Son+2q+eU/qdb72B+tqfyc4zMTqy8tCpF1qoiwXUrRASs0QDxX8bMnvfyAN9ZeYU GuteNEJ2vzlWngIeu180aTSlNNNm2onrJxG/chrtGetKEJWr7EhJuFfCJLgUy94g ORSCJ4jKr2FIBqFR1Nd++fPVjNEZD5fvv1Pji6qeytEDdDv2kPtSNERvoNpkm3r4e 4cm7ap659FPNAXDzm/k18V4D4tvZqCaEITDjFR552EAQNS-sung/UAq+VDC3LFU 6rkEnv= "Kigy"



PRIVATE KEY

##

a very large a very large

secret prime secret prime

number number

#### **PUBLIC KEY**



the product of those two very large prime numbers used to make the private key, which is very, very hard to reverse back









# × # =





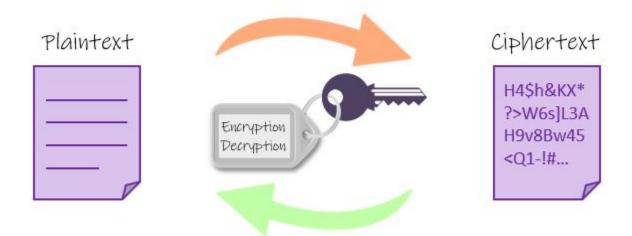
pubkey.asc

----BEGIN PGP PUBLIC KEY BLOCK---mQIHBFLQTTOBEACphIBxxsqLopI9PKLDulareUwA9HxXoVpxyoS+3H4VDyxjBB5QG go2ffn/bQAOyRAGa8panHxOBxQgJLI+A2eOOLBFHf5b3Q9FcCH7S+eb007xXAje zb6JL8bQ2xVMZT5AKIEGOHRDe+SySG2+F5GNYSYxHFRF/bogxyhfCTEabty jévgvigCSPxxkb1MBxx2gR0Cu6eNjK+J7512j2jpjebptVvK/4NjygK9Ayx5CLSFx DuELocuxcrUULoC7iNV9IBMVac8H/Y3KE7/mMCEITYn1hsim2h1//2mGdisnxikP kO+db&PefaLeUtAY+CT&ST0uSJWMy7iYwILblOvk9XIacc@BXIeiLcvi7OADAOAI LStoSzwjaKigAD/anzjqD4bMN;AAlczOyqczzU3LZb)VIzixka0jjf+q0X9bBaB dKhrEmLhJzxJT64GgonKtzylRCBfQS3l3fTUZxYSiRCtXxxfPRr/MAkrNZhto9Ujq vOVnBAlhvtNSDN1RJcvXUKvtdNQf1dOkxUANbe8FX3mc8c3P/2PtiEucXdxxY9qd vOVAALAD-tallEFB132 reVSIVAre-db052 didos GAMbel FI In el e 19 72 AFL Liste Montal Vigoria. 19 45 henitiga Vigoriana Historiana xE7TppGGgg7883w+cCbg+s9VGVgb2DA4k7v8EGCWGey71ee85gVCykhAp6ZNSC9Sbs

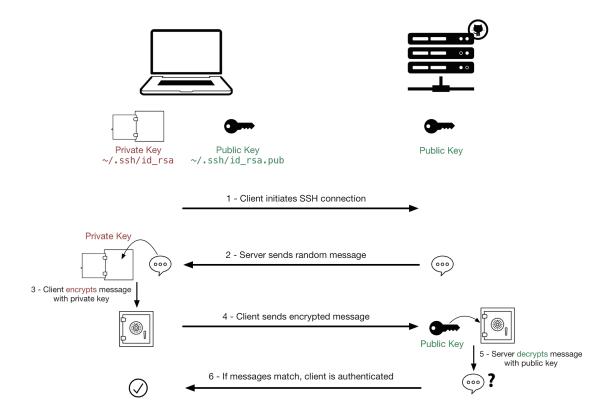
-- END POP PUBLIC KEY BLOCK-----

# COMPRENDRE L'ENCRYPTION SYMÉTRIQUE

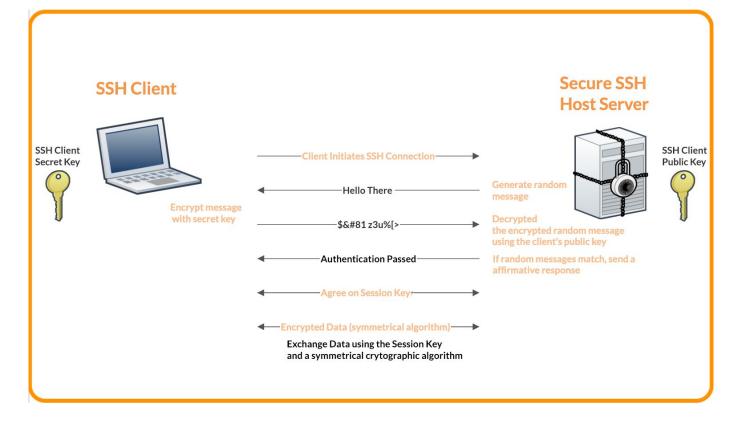
#### Symmetric Encryption



#### SSH AUTHENTIFICATION



### POUR RÉSUMER



#### UTILISATION DE SSH AVEC LOGIN / PASSWORD

- Le service SSH est actif par défaut sur votre carte Jetson Nano (mais pas sur votre VM)
- ssh username@ip
- Saisie du mot de passe
- Connexion à la machine
  - > ssh afauvel@192.168.64.201
    afauvel@192.168.64.201's password:
    Welcome to Ubuntu 18.04.6 LTS (GNU/L)

#### Inconvénients:

- Il faut saisir son mot de passe à chaque connexion
- Si on a mis un mot de passe peu complexe, la sécurité est faible
- Si le mot de passe est compromis, l'attaquant peut se connecter physiquement et via SSH à la machine

#### UTILISATION DE SSH AVEC DES CLEFS - GÉNÉRER SA CLEF

- Générer sa clef SSH

   (utiliser du chiffrement
   RSA et protéger la clef avec une passphrase)
- ssh-keygen -t rsa
  - nb : cette commande peut varier selon le système
  - nb2: Windows intègre désormais nativement la commande SSH
- Nous obtenons deux clefs
  - La clef privée qui ne doit jamais bouger de votre machine
  - La clef publique qui peut être librement partagée

```
afauvel@axel-jetson:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/afauvel/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/afauvel/.ssh/id_rsa.
Your public key has been saved in /home/afauvel/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:voNlaFTINFSIdeGd+qyR0Vr5MOuQAbPP0vPDtYcQrKq afauvel@axel-jetson
The kev's randomart image is:
+---[RSA 2048]----+
      *=++.
     . ++.. .
     0 0. 0
      +. 0.
     .o.oS.
     .++++*.
    ...B=@ooo
   E ..*+Xo .
       ..*0..
   -- [SHA256] --
```

#### UTILISATION DE SSH AVEC DES CLEFS - COPIER SA CLEF

- Option n°1: je connais le mot de passe de l'utilisateur avec lequel je souhaite me connecter
  - o ssh-copy-id username@ip

- > ssh-copy-id afauvel@192.168.64.201
  /usr/bin/ssh-copy-id: INFO: attempting to
  /usr/bin/ssh-copy-id: INFO: 2 key(s) remail
  afauvel@192.168.64.201's password:
- Number of key(s) added:

Now try logging into the machine, with: 'and check to make sure that only the key(s

- Option n°2 : je fournis ma clef à la personne responsable de déployer les clefs sur les machines
  - cat \$HOME/.ssh/id\_rsa.pub
  - J'envoie ça à la personne qui va la copier sur la machine

cat \$HOME/.ssh/id\_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2Cuo7+EciETjH7oousxo1Z10TP+fpDE;
BT46rElbh0szeKG8cD4rd68SV6s0MnxRWYIQRqcyNtFMUZ4e70XA2jXlwyLfpptBg/NMO1
JVbA9c6Psf5x8C4VQGUHXo1fYmg12U2n1MAvcx3V7GCW3r1HkJEgkd27wGuL0b46QGmcivIxL2/6nNZEep17yDC8vU1DDL18Sm0GWVfDWeX0r2+UCeU= afauvel@MC-C02C91YKMD6T

#### UTILISATION DE SSH AVEC DES CLEFS - SE CONNECTER

ssh username@ip

PAF chocapics

```
> ssh afauvel@192.168.64.201
Welcome to Ubuntu 18.04.6 LTS (GNU/L)

* Documentation: https://help.ubun.
 * Management: https://landscape
 * Support: https://ubuntu.com
```

This system has been minimized by ren

#### EXERCICE

- installez le paquet ssh
- connectez vous à votre VM depuis votre système en utilisant login/password (rappelez vous, lors de l'installation de la VM, nous avions fait une redirection de ports)
- Déconnectez vous de votre VM
- Générez une paire de clefs sur votre système
- Autorisez votre clef publique sur votre VM
- Connectez vous à votre VM en utilisant votre clef privée

#### POUR ALLER PLUS LOIN

```
Comment marche SSH:
<a href="https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ss">https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work</a>

Config SSH:
<a href="https://linuxize.com/post/using-the-ssh-config-file/">https://linuxize.com/post/using-the-ssh-config-file/</a>
```

Agent SSH: <a href="https://www.ssh.com/academy/ssh/agent">https://www.ssh.com/academy/ssh/agent</a>